Article 19

CLAIMS

1. (amended) A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating an intermediate key by using key information which is stored on a medium and in a recording/reproduction device for the medium, and using the intermediate key to generate a key with which to apply cryptographic processing to the content,

cryptographic processing means for applying cryptographic processing to the content by using the key, and

retention means for retaining the intermediate key in a form which is not recognizable as a key.

2. (amended) The copyright protective device according to claim 1, wherein,

the key generation means generates said key with respect to each of a plurality of media,

the cryptographic processing means applies cryptographic processing to the content by using the key generated for each medium, and

the retention means retains the intermediate keys generated for the plurality of media in a form which is not recognizable as a key.

3. The copyright protective device according to claim 1, wherein the retention means retains the intermediate key and the

key in a storage circuit within integrated circuitry.

4. (amended) A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating an intermediate key by using key information which is stored on a medium and in a recording/reproduction device for the medium, and using the intermediate key to generate a key with which to apply cryptographic processing to the content,

cryptographic processing means for applying cryptographic processing to the content by using the key, and

retention means for retaining the intermediate key in an encrypted manner.

5. (amended) The copyright protective device according to claim 4, wherein,

the key generation means generates said key with respect to each of a plurality of media,

the cryptographic processing means applies cryptographic processing to the content by using the key generated for each medium, and

the retention means retains the intermediate keys generated for the plurality of media in an encrypted manner.

6. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and an intermediate

key for generating the key, by sequentially extracting necessary data from key generation data which is formed in a matrix and applying computation processing thereto,

cryptographic processing means for applying cryptographic processing to the content by using the key, and

retention means for retaining at least one of the intermediate key and the key generation data.

7. The copyright protective device according to claim 6, wherein,

the key generation means generates said key with respect to each of a plurality of media,

the cryptographic processing means applies cryptographic processing to the content by using the key generated for each medium, and

the retention means retains the intermediate key and the key generation data with respect to each medium.

8. (amended) A copyright protective method for encrypting or decrypting a content, comprising:

a key generation step of generating an intermediate key by using key information which is stored on a medium and in a recording/reproduction device for the medium, and using the intermediate key to generate a key with which to apply cryptographic processing to the content,

an cryptographic processing step of applying cryptographic processing to the content by using the key, and

a retention step of retaining the intermediate key in a form which is not recognizable as a key.

9. (amended) The copyright protective method according to claim 8, wherein,

the key generation step generates said key with respect to each of a plurality of media,

the cryptographic processing step applies cryptographic processing to the content by using the key generated for each medium, and

the retention step retains the intermediate keys generated for the plurality of media in a form which is not recognizable as a key.

10. (amended) A copyright protective method for encrypting or decrypting a content, comprising:

a key generation step of generating an intermediate key by using key information which is stored on a medium and in a recording/reproduction device for the medium, and using the intermediate key to generate a key with which to apply cryptographic processing to the content,

an cryptographic processing step of applying cryptographic processing to the content by using the key, and

a retention step of retaining the intermediate key in an encrypted manner.

11. A copyright protective method for encrypting or decrypting a content, comprising:

a key generation step of generating a key with which to apply cryptographic processing to the content and an intermediate key for generating the key, by sequentially extracting necessary data from key generation data which is formed in a matrix and applying computation processing thereto,

an cryptographic processing step of applying cryptographic processing to the content by using the key, and

a retention step of retaining at least one of the intermediate key and the key generation data.

12. The copyright protective method according to claim 11, wherein,

the key generation step generates said key with respect to each of a plurality of media,

the cryptographic processing step applies cryptographic processing to the content by using the key generated for each medium, and

the retention step retains the intermediate key and the key generation data with respect to each medium.

13. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and

cryptographic processing means, to which a content

containing identification information indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification information by using the key, and for outputting a result of the cryptographic processing,

wherein the cryptographic processing means restrains the result of the cryptographic processing from being outputted when the notification signal indicates that key generation is being performed.

14. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not,

cryptographic processing means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing, and

selection means for selecting a content which is inputted to the cryptographic processing means when the notification signal indicates that key generation is being performed, and otherwise selecting the result of the cryptographic processing

outputted from the cryptographic processing means.

15. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and

cryptographic processing means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing,

wherein, when the notification signal indicates that key generation is being performed, the cryptographic processing means switches an input enable signal for controlling inputting of contents to an input disabled state.

16. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content, and

cryptographic processing means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the

identification signal by using the key, and for outputting a result of the cryptographic processing,

wherein, when key generation is being performed, the key generation means switches an input enable signal for controlling inputting of contents to an input disabled state.

17. A signal processing device for processing an input signal containing per plurality of symbols a heading pattern which represents a heading of a processing unit, comprising:

a register for retaining the input signal which is sequentially inputted,

heading pattern detection means for detecting the heading pattern being contained in the input signal retained in the register,

signal processing means for applying predetermined signal processing to the input signal which is supplied via the register, and notifying whether the input signal is being processed or not, and

control signal generation means which outputs a reset signal to the signal processing means if the signal processing means is not performing processing when the heading pattern is detected by the heading pattern detection means, and if the signal processing means is performing processing when the heading pattern is detected by the heading pattern detection means, switches an input enable signal for controlling input to an input disabled state and transitions to a reset-waiting state, and

outputs a reset signal to the signal processing means when the processing by the signal processing means is completed in the reset-waiting state.

18. A signal processing device for processing an input signal which is inputted symbol by symbol in accordance with an input enable signal,

signal processing means to which not more than c symbols of said input signal is inputted after the input enable signal changes to an input disabled state, wherein the signal processing means processes b symbols of said signal at one time and notifies an overflow state of internal processing,

input enable signal generation means for switching the input enable signal to an input disabled state when the processing by the signal processing means enters an overflow state, and

a register which retains a symbols of said input signal, outputs b symbols to the signal processing means when the input enable signal is in an input enabled state, wherein a, b, and c are of the relationship $a \geqq (b+c)$, and employs as a load signal a logical OR signal between the input enable signal and a signal obtained by delaying the signal by one clock cycle.

19. A signal processing device for processing an input signal which is inputted symbol by symbol in accordance with an input enable signal,

signal processing means to which not more than c symbols of said input signal is inputted after the input enable signal

changes to an input disabled state, wherein the signal processing means applies predetermined processing to the input signal and notifies whether the input signal is acceptable or not,

a memory for storing the input signal and outputting the stored input signal to the signal processing means,

memory control means which, if the input signal is acceptable to the signal processing means, controls the memory so that the data is read therefrom, and outputs a write address and a read address while performing write control so as not to overwrite data on any unread data, and

input enable signal generation means for switching the input enable signal to an input disabled state when a write margin which is calculated based on the write address and the read address outputted from the memory control means reaches at least c symbols.